

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application : **10/531,939**
Applicant(s) : **KAMPERMAN et al.**
Filed : **4/19/2005**
Confirmation : **4488**
T.C./Art Unit : **2431**
Examiner : **VAUGHAN, Michael R.**
Atty. Docket : **NL021063US**

Title: **METHOD AND DEVICE FOR AUTHORIZING CONTENT OPERATIONS**

Mail Stop: **APPEAL BRIEF - PATENTS**
Commissioner for Patents
Alexandria, VA 22313-1450

APPEAL UNDER 37 CFR 41.37

Sir:

This is an appeal from the decision of the Examiner dated 20 July 2009, finally rejecting claims 1-21 and 31-32 of the subject application.

This paper includes (each beginning on a separate sheet):

- 1. Appeal Brief;**
- 2. Claims Appendix;**
- 3. Evidence Appendix; and**
- 4. Related Proceedings Appendix.**

APPEAL BRIEF

I. REAL PARTY IN INTEREST

The above-identified application is assigned, in its entirety, to
Koninklijke Philips Electronics N. V.

II. RELATED APPEALS AND INTERFERENCES

Appellant is not aware of any co-pending appeal or interference that will directly affect, or be directly affected by, or have any bearing on, the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 22-30 are canceled.

Claims 1-21 and 31-32 are pending in the application.

Claims 1-3, 5-6, 8-10, 12-13, and 31 stand rejected by the Examiner under 35 U.S.C. 102(b).

Claims 4, 7, 11, 14-21, and 32 stand rejected by the Examiner under 35 U.S.C. 103(a).

These rejected claims are the subject of this appeal.

IV. STATUS OF AMENDMENTS

No amendments were filed subsequent to the final rejection in the Office Action dated 20 July 2009.

V. SUMMARY OF CLAIMED SUBJECT MATTER¹

The invention addresses the granting of rights among a domain of users, such as a family domain (applicants' specification, page 4, lines 1-4). Rights are distinguished as content rights and user rights. Content rights provide rights that permit a device to perform one or more operations on content material; for example, providing a decryption key allows a device to access encrypted material. A user right enables a user to use the content right (page 4, lines 23-28). In an embodiment of this invention, if any member of a domain obtains a content right, all members of the domain have that content right (page 4, lines 6-9).

For example, if one member of a family purchases permission to access a particular content item (a user right), another member of the family can be granted access to that material by providing proof that he or she is in the same family as the member having the user right. Of particular note, the member who purchased the content right does not have to expressly grant the shared right to the requesting member; the requesting member need only show that the purchasing member has the content right and provide proof of membership in the same domain as the purchasing member (page 5, lines 10-18, the 'first' user being the requesting member, and the 'second' user being the purchasing member; see also page 10, lines 7-17).

An example proof of membership is a domain certificate issued by a trusted third party (page 9, lines 15-23. The domain certificate may be issued to each member of the domain, or a single domain certificate listing all members of the domain may be issued (page 10, lines 1-14).

¹ It is respectfully noted that it is not the appellants' intention that the claimed embodiments of this invention be limited to operation within the example embodiments described in this brief, beyond what is required by the claim language. These examples and their description are provided to facilitate ease of understanding and to comply with the requirements of an appeal brief, without intending that any further interpreted limitations be read into the claims as presented.

As claimed in independent claim 1, the invention comprises a method of authorizing an operation on a machine requested by a first user on a content item comprising:

receiving, at the machine, a user right certificate that identifies a second user and authorizes the second user to perform the requested operation on the content item (page 5, lines 10-13; page 10, line12, UR1 of FIG. 3), and

authorizing the operation on the machine by the first user upon receipt of information from the first user that links the first user and the second user as members of a common authorized domain (page 5, lines 13-18; page 10, lines 13-14, DC1 and DC2 of FIG. 3).

As claimed in independent claim 8, the invention comprises a device arranged to perform an operation requested by a first user on a content item comprising:

a receiving unit that is configured to receive a user right certificate that identifies a second user and authorizes the second user to perform the requested operation on the content item (page 5, lines 10-13; page 10, line12, UR1 of FIG. 3), and

an authorization unit that is configured to authorize the operation upon receipt of information from the first user that links the first user and the second user as members of a common authorized domain (page 5, lines 13-18; page 10, lines 13-14, DC1 and DC2 of FIG. 3; page 10, lines 1-6).

As claimed in dependent claims 2 and 9, the information from the first user comprises one or more domain certificates identifying the first and second users as members of the authorized domain (page 10, lines 1-14).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-3, 5-6, 8-10, 12-13, and 31 stand rejected under 35 U.S.C. 102(b) over Jonsson (WO 01/76294).

Claims 4 and 11 stand rejected under 35 U.S.C. 103(a) over Jonsson.

Claims 7 and 21 stand rejected under 35 U.S.C. 103(a) over Jonsson in view of Messerges et al. (USPA 2002/0157002, hereinafter Messerges).

Claims 14 and 32 stand rejected under 35 U.S.C. 103(a) over Jonsson in view of Saw et al. (USP 7,020,781, hereinafter Saw).

Claims 15-17 and 19 stand rejected under 35 U.S.C. 103(a) over Jonsson in view of Wyman (USP 5,204,897).

Claim 18 stands rejected under 35 U.S.C. 103(a) over Jonsson and Wyman in view of Moskowitz et al. (WO 01/18628, hereinafter Moskowitz).

Claim 20 stands rejected under 35 U.S.C. 103(a) over Jonsson in view of Kahn et al. (USP 6,135,646, hereinafter Kahn).

VII. ARGUMENT

Claims 1-3, 5-6, 8-10, 12-13, and 31 stand rejected under 35 U.S.C. 102(b) over Jonsson

MPEP 2131:

"A claim is anticipated only if **each and every element** as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)... "The **identical invention** must be shown in as **complete detail** as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Claims 1-3, 5-6, 8-10, 12-13, and 31

Jonsson fails to teach receiving a user right certificate that authorizes a second user to perform an operation requested by a first user, and fails to teach authorizing the operation by the first user upon receipt of information that links the first user and the second user as members of a common authorized domain, as specifically claimed in each of the applicants' independent claims 1 and 8, upon which all the other pending claims depend.

The Examiner asserts that Jonsson teaches receiving a user right certificate that authorizes a second user to perform an operation requested by a first user, and authorizing the operation by the first user upon receipt of information at column 7, lines 27-35 (Office action, page 5, last partial paragraph). This assertion is incorrect.

At the cited text, Jonsson teaches:

"A user can preferably access a client structure, to which he is assigned, by means of a computer or a telephone. In case of a computer, the user can visit on the Internet a web site of the access provider. After a login procedure, including stating some sort of personal identification code, the user will come to a private homepage. On this private homepage he will be able to see what services are available and, preferably, which level of authority he has to the different services." (Jonsson, page 7, lines 27-35.)

As is clearly evident, the cited text does not address receiving a user right certificate of another user to authorize a request by a requesting user, as specifically claimed by the applicants.

The Examiner also asserts that Jonsson teaches receiving information from the requesting user that links the requesting user and the other user as members of a common authorized domain at page 2, lines 30-33² (Office action, page 6, line 1). This assertion is also incorrect.

At the cited text, Jonsson teaches:

"Each client structure has at least one assigned user. A first user in a first client structure is provided with the ability to give a second user assigned to a second client structure authority to access said first client structure." (Jonsson, page 2, lines 30-33.)

As is clearly evident, the cited text does not address receiving linking information from the requesting user, as specifically claimed by the applicants. In Jonsson, the granting of rights is explicit, at the discretion of the user who is initially granted the right. In Jonsson, a user is authorized to grant access to another user, but this grant must be explicitly provided by the granting user. If a user in Jonsson has not been explicitly granted access, that user must first contact the user who is initially granted the right, and have that user initiate the grant. Only after the user who is initially granted the right has initiated the grant can the second user's request be authorized.

² line 43, cited in the Office action, does not exist on page 2 of Jonsson; the applicants assume that line 33 is the proper cite.

The Examiner acknowledges that the granting of rights in Jonsson is explicit, and references page 4, lines 14-18, noting that both users are registered with the access provider:

"The access provider gives service providers, such as companies, the possibility to interact with the service platform and to offer services to clients registered with the access provider." (Jonsson, page 4, lines 14-18.)

In the applicants' claimed invention, an explicit granting and registering of rights to each user is not required. Only one user right is required, along with information that links the requesting user to the authorized user as members of a common domain. Jonsson does not teach or suggest using the rights of one user to authorize the right by another user by showing that the two users are members of the same authorized domain, as specifically claimed in each of the applicants' independent claims.

Because Jonsson fails to teach receiving a user right certificate that authorizes a second user to perform an operation requested by a first user, and fails to teach authorizing the operation by the first user upon receipt of information that links the first user and the second user as members of a common authorized domain, the applicants respectfully maintain that the rejection of claims 1-3, 5-6, 8-10, 12-13, and 31 under 35 U.S.C. 102(b) over Jonsson is unfounded, and should be reversed by the Board.

Claims 2-3, 6, 9-10, and 12-13

Jonsson does not teach that the information provided by the requesting user comprises one or more domain certificates identifying the first and second users as members of the authorized domain, as specifically claimed in claims 2 and 9, upon which claims 3-4, 6-7, 10-21, and 32 depend.

The Examiner asserts that Jonsson's client structure corresponds to a domain certificate that is provided by the requesting user. This assertion is incorrect.

The applicants define a domain certificate at page 9, lines 15-24, as a certificate that is issued by a trusted third party that defines the persons or entities belonging to a domain. The applicants also teach and claim that this certificate is transportable, and provided to the authorizing machine/device by the requesting user.

Jonsson's client structure is a structure within the authorizing machine/device that lists all authorized users. This structure is not transportable by a user, and in particular, is not a certificate that is issued by a trusted third party, and is not submitted to the authorizing machine/device by a requesting user.

Because Jonsson does not teach that the information provided by the requesting user comprises one or more domain certificates identifying the first and second users as members of the authorized domain, the applicants respectfully maintain that the rejection of claims 2-3, 6, 9-10, and 12-13 under 35 U.S.C. 102(b) over Jonsson is unfounded, and should be reversed by the Board.

Claims 4 and 11 stand rejected under 35 U.S.C. 103(a) over Jonsson

**Claims 7 and 21 stand rejected under 35 U.S.C. 103(a)
over Jonsson in view of Messerges**

**Claims 14 and 32 stand rejected under 35 U.S.C. 103(a)
over Jonsson in view of Saw**

**Claims 15-17 and 19 stand rejected under 35 U.S.C. 103(a)
over Jonsson in view of Wyman**

**Claim 18 stands rejected under 35 U.S.C. 103(a) over
Jonsson and Wyman in view of Moskowitz**

**Claim 20 stands rejected under 35 U.S.C. 103(a)
over Jonsson in view of Kahn**

Claims 4, 7, 11, 14-17, 19, 21, and 32

Each of the above rejected claims is dependent upon claim 1 or claim 8, and in these rejections, the Examiner relies on Jonsson for teaching the elements of claims 1 and 8. As noted above, Jonsson fails to teach the elements of claims 1 and 8, and neither Messerges, Saw, Wyman, Moskowitz, nor Kahn cures this deficiency. Accordingly, the applicants respectfully maintain that the rejections of claims 4, 7, 11, 14-17, 19, 21, and 32 under 35 U.S.C. 103(a) that rely on Jonsson for teaching the elements of claims 1 and 8 are unfounded, and should be reversed by the Board.

Further, each of the above rejected claims is dependent upon claim 2 or claim 9, and in these rejections, the Examiner relies on Jonsson for teaching the elements of claims 2 and 9. As noted above, Jonsson fails to teach the elements of claims 2 and 9, and neither Messerges, Saw, Wyman, Moskowitz, nor Kahn cures this deficiency, and the Examiner does not rely on these references for these teachings. Accordingly, the applicants respectfully maintain that the rejections of claims 4, 7, 11, 14-17, 19, 21, and 32 under 35 U.S.C. 103(a) that rely on Jonsson for teaching the elements of claims 2 and 9 are unfounded, and should be reversed by the Board.

CONCLUSIONS

Because Jonsson fails to teach receiving a user right certificate that authorizes a second user to perform an operation requested by a first user, and fails to teach authorizing the operation by the first user upon receipt of information that links the first user and the second user as members of a common authorized domain, the applicants respectfully request that the Examiner's rejection of claims 1-3, 5-6, 8-10, 12-13, and 31 under 35 U.S.C. 102(b) and claims 4, 7, 11, 14-17, 19, 21, and 32 under 35 U.S.C. 103(a) be reversed by the Board, and the claims be allowed to pass to issue.

Because Jonsson does not teach that the information provided by the requesting user comprises one or more domain certificates identifying the first and second users as members of the authorized domain, the applicants respectfully request that the rejection of claims 2-3, 6, 9-10, and 12-13 under 35 U.S.C. 102(b) and claims 4, 7, 11, 14-17, 19, 21, and 32 under 35 U.S.C. 103(a) be reversed by the Board, and the claims be allowed to pass to issue.

Respectfully submitted,

/Robert M. McDermott/
Robert M. McDermott, Esq.
Reg. 41,508
804-493-0707
for: Kevin C. Ecker
Reg. 43,600
914-333-9618

Please direct all correspondence to:
Corporate Counsel
PHILIPS IP&S
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
914-332-0222

CLAIMS APPENDIX

1. A method of authorizing an operation on a machine requested by a first user on a content item comprising:
 - receiving, at the machine, a user right certificate that identifies a second user and authorizes the second user to perform the requested operation on the content item, and
 - authorizing the operation on the machine by the first user upon receipt of information from the first user that links the first user and the second user as members of a common authorized domain.
2. The method of claim 1, wherein the information comprises one or more domain certificates identifying the first and second users as members of the authorized domain.
3. The method of claim 2, wherein the one or more domain certificates comprise a first domain certificate identifying the first user as a member of the authorized domain, and a second domain certificate identifying the second user as a member of the authorized domain.
4. The method of claim 2, wherein the one or more domain certificates comprise a single certificate identifying the first and second users as members of the authorized domain.
5. The method of claim 1, wherein the operation comprises at least one of: a rendering of the content item, a recording of the content item, a transfer of the content item and a creation of a copy of the content item.

6. The method of claim 2, comprising receiving a content right containing necessary information for performing the requested operation on the content item, the user right certificate of the second user authorizing the second user to perform the requested operation using the content right.
7. The method of claim 6, wherein the operation is not authorized if the content right does not identify the authorized domain.
8. A device arranged to perform an operation requested by a first user on a content item comprising:
 - a receiving unit that is configured to receive a user right certificate that identifies a second user and authorizes the second user to perform the requested operation on the content item, and
 - an authorization unit that is configured to authorize the operation upon receipt of information from the first user that links the first user and the second user as members of a common authorized domain.
9. The device of claim 8, wherein the information comprises one or more domain certificates identifying the first and second users as members of the authorized domain.
10. The device of claim 9, wherein the one or more domain certificates comprise a first domain certificate identifying the first user as a member of the authorized domain, and a second domain certificate identifying the second user as a member of the authorized domain.
11. The device of claim 9, wherein the one or more domain certificates comprise a single certificate identifying the first and second users as members of the authorized domain.

12. The device of claim 9, being arranged to receive an identifier for the first user from an identification device and to perform the operation if the received identifier matches the identification of the first user in the one or more domain certificates.
13. The device of claim 8 or 9, being arranged to receive a content right containing necessary information for performing the requested operation on the content item, the user right certificate of the second user authorizing the second user to perform the requested operation using the content right.
14. The device of claim 11, wherein at least a portion of the content right is encrypted using an encryption key for which a corresponding decryption key is available to the device.
15. The device of claim 13, wherein the content right is provided with a digital signature allowing verification of the authenticity of the content right.
16. The device of claim 15, being arranged to perform the operation if the digital signature can be verified successfully using a digital certificate associated with an authorized content provider.
17. The device of claim 15, being arranged to perform the operation if the digital signature can be verified successfully using a digital certificate associated with a particular device.
18. The device of claim 15, being arranged to refuse to perform the operation if the digital signature cannot be verified successfully using a digital certificate associated with an authorized content provider and a digital watermark associated with the authorized content provider is present in the content item.

19. The device of claim 15, being arranged to extract a public key from the content right and to use the extracted public key in determining whether the operation is authorized.

20. The device of claim 13, being arranged to determine a robust fingerprint for the content item and to refuse to perform the operation if the determined robust fingerprint does not match a robust fingerprint comprised in the content right.

21. The device of claim 9, being arranged to receive a content right containing necessary information for performing the requested operation on the content item, the user right certificate of the second user authorizing the second user to perform the requested operation using the content right, and to refuse to perform the operation if the authorized domain is not identified by the content right.

22-30 (Canceled)

31. The method of claim 1, comprising receiving a content right containing necessary information for performing the requested operation on the content item, the user right certificate of the second user authorizing the second user to perform the requested operation using the content right.

32. The device of claim 13, being arranged to extract a public key from the content right and to use the extracted public key in determining whether the operation is authorized.

EVIDENCE APPENDIX

No evidence has been submitted that is relied upon by the appellant in this appeal.

RELATED PROCEEDINGS APPENDIX

Appellant is not aware of any co-pending appeal or interference which will directly affect or be directly affected by or have any bearing on the Board's decision in the pending appeal.